

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

1-639 U.S. PTO
09/504293
02/15/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 2月26日

出 願 番 号
Application Number:

平成11年特許願第049346号

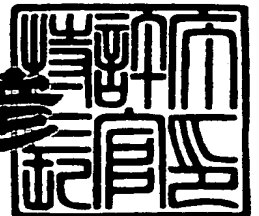
出 願 人
Applicant(s):

沖電気工業株式会社

1999年12月24日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特平11-3091107

【書類名】 特許願
【整理番号】 SA003369
【あて先】 特許庁長官殿
【国際特許分類】 G06F 12/00
G06F 17/30

【発明者】

【住所又は居所】 東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社
社内

【氏名】 中沢 修

【特許出願人】

【識別番号】 000000295

【氏名又は名称】 沖電気工業株式会社

【代理人】

【識別番号】 100082050

【弁理士】

【氏名又は名称】 佐藤 幸男

【選任した代理人】

【識別番号】 100102923

【弁理士】

【氏名又は名称】 加藤 雄二

【手数料の表示】

【予納台帳番号】 058104

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9100477

【包括委任状番号】 9500200

特平 1 1 - 0 4 9 3 4 6

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 分散ディレクトリ管理システム

【特許請求の範囲】

【請求項 1】 複数のサービス空間で管理されるサービスオブジェクトの検索サービスを提供するためのシステムであって、サービス空間集中管理機構と、サービスオブジェクト管理機構と、サービス空間接続管理機構と、サービスオブジェクト検索管理機構とを備え、

前記サービス空間集中管理機構は、前記複数のサービス空間の相互接続情報を前記サービス空間接続管理機構から収集して管理し、

前記サービスオブジェクト管理機構は、所属するサービス空間において、サービス利用者が検索の対象とする前記サービスオブジェクトや属性情報を記憶したオブジェクトリポジトリを管理してその検索を実行し、

前記サービス空間接続管理機構は、前記サービスオブジェクト管理機構とメッセージ通信を行い、担当するサービス空間と他のサービス空間との相互接続情報を収集して管理し、

サービスオブジェクト検索管理機構は、前記サービス利用者の検索メッセージを前記サービスオブジェクト管理機構に送信して、該当するサービスオブジェクトの検索を依頼し、前記サービスオブジェクト管理機構の検索結果を受け付けて、その内容を解釈し前記サービス利用者へ送信するメッセージを生成することを特徴とする分散ディレクトリ管理システム。

【請求項 2】 請求項 1 に記載の分散ディレクトリ管理システムにおいて、前記サービスオブジェクト管理機構は、自己の状態が変化する度に、自己が所属するサービス空間を担当する前記サービス空間接続管理機構に対して、自己の存在を示すメッセージを送信し、

前記サービス空間接続管理機構は、前記サービスオブジェクト管理機構のメッセージを受信して、担当するサービス空間と他のサービス空間との相互接続情報を更新することを特徴とする分散ディレクトリ管理システム。

【請求項 3】 請求項 1 に記載の分散ディレクトリ管理システムにおいて、前記サービスオブジェクト管理機構は、一定時間おきに、自己が所属するサー

ビス空間を担当する前記サービス空間接続管理機構に対して、自己の存在を示すメッセージを送信し、

前記サービス空間接続管理機構は、前記サービスオブジェクト管理機構のメッセージを受信して、担当するサービス空間と他のサービス空間との相互接続情報を更新することを特徴とする分散ディレクトリ管理システム。

【請求項4】 請求項2または3に記載の分散ディレクトリ管理システムにおいて、

前記サービスオブジェクト管理機構は、マルチキャストアナウンス機能を用いて、前記サービス空間接続管理機構に対して、自己の存在を示すメッセージを送信し、

前記サービス空間接続管理機構は、前記サービスオブジェクト管理機構のメッセージを受信して、担当するサービス空間と他のサービス空間との相互接続情報を更新することを特徴とする分散ディレクトリ管理システム。

【請求項5】 請求項1に記載の分散ディレクトリ管理システムにおいて、前記サービスオブジェクト検索管理機構は、前記サービス利用者から検索を依頼する旨のメッセージを受け付けたとき、サービス空間接続管理機構の持つ前記相互接続情報を利用して、検索メッセージを、自サービス空間と共に、所定の他のサービス空間に送信して検索依頼を行うことを特徴とする分散ディレクトリ管理システム。

【請求項6】 請求項1に記載の分散ディレクトリ管理システムにおいて、ディレクトリサービスを利用するためのチケットをサービス利用者に発行し、前記利用者からチケットの提出があった場合、その正当性を検証して、前記サービスオブジェクト検索管理機構によるアクセスを許可するディレクトリ管理認証機構を備えたことを特徴とする分散ディレクトリ管理システム。

【請求項7】 請求項1に記載の分散ディレクトリ管理システムにおいて、サービス利用者からデジタル署名された検索依頼メッセージを受け付けた場合、その正当性を検証して、前記サービスオブジェクト検索管理機構によるアクセスを許可するディレクトリ管理認証機構を備えたことを特徴とする分散ディレクトリ管理システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、インターネット等の複雑なネットワーク環境下で、ネットワーク構成の変更に対応しつつ様々なサービスオブジェクトの検索や管理を可能にする分散ディレクトリ管理システムに関する。

【0 0 0 2】

【従来の技術】

インターネットや大規模なイントラネットのような複雑なネットワーク環境下で様々な情報を検索する場合には、これらの情報を管理しアクセスするシステムが必要になる。そのためのシステムをディレクトリ管理システムと呼び、このようなシステムを利用者に提供するためにディレクトリサービスが存在する。ディレクトリサービスの一例として、TCP/IPネットワークにおけるホスト名とIPアドレスとの対応を記録管理する“hosts”ファイルやDNS（ドメインネームシステム）が知られている。これらは一種のデータベースファイルに名前管理機能を付加したものである。

【0 0 0 3】

これらは広義のディレクトリサービスであるが、CCITTにより策定されたものに、X.500と呼ばれるディレクトリサービスがある。これは、ディレクトリの分散配置／階層管理／複製管理等のプロトコルや構造等を規定しており、各種のネットワークリソースをオブジェクト指向概念により管理する。ここでいうネットワークリソースは、ディレクトリに関する情報のことである。X.500によるディレクトリサービスは、分散オペレーティングシステムや分散処理用ミドルウェア等で広く採用されている。

【0 0 0 4】

X.500では、利用者がディレクトリサービスに接続して、ディレクトリ内のサービスオブジェクトを検索／変更する場合に、DAP（ディレクトリアクセスプロトコル）と呼ばれるプロトコルを利用する。サービスオブジェクトとは、利用者が検索しようとする情報のことである。更に、DAPの問題点を解決し軽量化

したLDAP（ライトウエイトディレクトリアクセスプロトコル）が出現し、多くのディレクトリサービスのアクセスプロトコルとして用いられている。

【0005】

例えば、米国マイクロソフト社のウィンドウズNT5.0から導入されるアクティブディレクトリ機能や米国ネットスケープ社のネットスケープディレクトリサーバにおいてもLDAPが用いられている。

【0006】

【発明が解決しようとする課題】

ところで、上記のような従来技術には次のような解決すべき課題があった。

ネットワークの運用時には、様々な環境の変化に応じてディレクトリサービスに利用されるネットワークリソース即ちネットワークディレクトリに関する情報の追加、削除、更新による変更が行われる。これらの変更に対応するディレクトリサービスの運用管理は手作業で行われており、多くの手数が要求される。

【0007】

また、それぞれ独自のサービス空間を持つネットワークが相互に連携するためのディレクトリサービスをディレクトリ間の階層管理機能と呼んでいるが、あるサービス空間の利用者が目的とするサービスオブジェクトを検索しようとする場合には、予めディレクトリ間の階層構造を知って、その構造に応じた検索処理が必要となる。即ち、利用者がディレクトリ間の階層構造を意識しなければ適切な検索が行われないという問題があった。

【0008】

また、こうした大規模な広域分散環境でネットワークを活用しようとする場合に、サービス空間毎に、特定の権限を有する利用者のみに検索／利用等の権利を与える仕組みが必要になる。従来のディレクトリサービスプロトコルには、こうした要求を満たす機能が十分に整備されていない。

【0009】

【課題を解決するための手段】

本発明は以上の点を解決するため次の構成を採用する。

＜構成1＞

複数のサービス空間で管理されるサービスオブジェクトの検索サービスを提供するためのシステムであって、サービス空間集中管理機構と、サービスオブジェクト管理機構と、サービス空間接続管理機構と、サービスオブジェクト検索管理機構とを備え、上記サービス空間集中管理機構は、上記複数のサービス空間の相互接続情報を上記サービス空間接続管理機構から収集して管理し、上記サービスオブジェクト管理機構は、所属するサービス空間において、サービス利用者が検索の対象とする上記サービスオブジェクトや属性情報を記憶したオブジェクトリポジトリを管理してその検索を実行し、上記サービス空間接続管理機構は、上記サービスオブジェクト管理機構とメッセージ通信を行い、担当するサービス空間と他のサービス空間との相互接続情報を収集して管理し、サービスオブジェクト検索管理機構は、上記サービス利用者の検索メッセージを上記サービスオブジェクト管理機構に送信して、該当するサービスオブジェクトの検索を依頼し、上記サービスオブジェクト管理機構の検索結果を受け付けて、その内容を解釈し上記サービス利用者に送信するメッセージを生成することを特徴とする分散ディレクトリ管理システム。

【0010】

〈構成2〉

構成1に記載の分散ディレクトリ管理システムにおいて、上記サービスオブジェクト管理機構は、自己の状態が変化する度に、自己が所属するサービス空間を担当する上記サービス空間接続管理機構に対して、自己の存在を示すメッセージを送信し、上記サービス空間接続管理機構は、上記サービスオブジェクト管理機構のメッセージを受信して、担当するサービス空間と他のサービス空間との相互接続情報を更新することを特徴とする分散ディレクトリ管理システム。

【0011】

〈構成3〉

構成1に記載の分散ディレクトリ管理システムにおいて、上記サービスオブジェクト管理機構は、一定時間おきに、自己が所属するサービス空間を担当する上記サービス空間接続管理機構に対して、自己の存在を示すメッセージを送信し、上記サービス空間接続管理機構は、上記サービスオブジェクト管理機構のメッセ

ージを受信して、担当するサービス空間と他のサービス空間との相互接続情報を更新することを特徴とする分散ディレクトリ管理システム。

【0012】

〈構成4〉

構成2または3に記載の分散ディレクトリ管理システムにおいて、上記サービスオブジェクト管理機構は、マルチキャストアナウンス機能を用いて、上記サービス空間接続管理機構に対して、自己の存在を示すメッセージを送信し、上記サービス空間接続管理機構は、上記サービスオブジェクト管理機構のメッセージを受信して、担当するサービス空間と他のサービス空間との相互接続情報を更新することを特徴とする分散ディレクトリ管理システム。

【0013】

〈構成5〉

構成1に記載の分散ディレクトリ管理システムにおいて、上記サービスオブジェクト検索管理機構は、上記サービス利用者から検索を依頼する旨のメッセージを受け付けたとき、サービス空間接続管理機構の持つ上記相互接続情報を利用して、検索メッセージを、自サービス空間と共に、所定の他のサービス空間に送信して検索依頼を行うことを特徴とする分散ディレクトリ管理システム。

【0014】

〈構成6〉

構成1に記載の分散ディレクトリ管理システムにおいて、ディレクトリサービスを利用するためのチケットをサービス利用者が発行し、上記利用者からチケットの提出があった場合、その正当性を検証して、上記サービスオブジェクト検索管理機構によるアクセスを許可するディレクトリ管理認証機構を備えたことを特徴とする分散ディレクトリ管理システム。

【0015】

〈構成7〉

構成1に記載の分散ディレクトリ管理システムにおいて、サービス利用者からデジタル署名された検索依頼メッセージを受け付けた場合、その正当性を検証して、上記サービスオブジェクト検索管理機構によるアクセスを許可するディレ

クトリ管理認証機構を備えたことを特徴とする分散ディレクトリ管理システム。

【0016】

【発明の実施の形態】

以下、本発明の実施の形態を具体例を用いて説明する。

〈具体例1〉

図1は、本発明による具体例1の分散ディレクトリ管理システム主要部構成図である。

図のシステムは、サービス空間集中管理機構10と、サービスオブジェクト検索管理機構20と、サービスオブジェクト管理機構30と、サービス空間接続管理機構40によりディレクトリ管理を行う。オブジェクトリポジトリ1は、実際にサービス利用者が検索の対象とするサービスオブジェクト3や属性情報5を記憶したデータベースである。

【0017】

サービスオブジェクトというのは、データファイルやプログラム等、ネットワークを通じて検索され参照される様々な情報により構成される。属性情報5は、各サービスオブジェクト3に付加されてその検索等を容易にするために利用されるキーワードやその他の情報から成る。即ち、サービス利用者は、属性情報5中に含まれる検索キーを用いてネットワーク上のサービスオブジェクトを検索し、これを利用する。

【0018】

分散ネットワーク環境では、このようなサービスオブジェクトを提供するサービス空間が多数存在する。この具体例では、オブジェクトリポジトリ1に記憶されたサービスオブジェクト3と属性情報5を管理し検索を実行するために、サービスオブジェクト管理機構30が設けられている。

【0019】

なお、図1を用いて説明したような各機構や機構内の様々な機能部は、それぞれ、例えばJ A V A言語環境のインスタンスオブジェクトとして表現されるソフトウェアにより実現される。そして、各機構は、それぞれオブジェクト間のメッセージ通信によって必要な情報を交換し、各機能を実現するように構成されてい

る。

【0 0 2 0】

図 2 には、複数のサービス空間をサービス対象とする分散ディレクトリ管理システム全体の構成図を示す。

図に示すように、サービス空間集中管理機構 1 0 は、複数のサービス空間 7 A，7 B，7 Cを一括して集中的に管理する機構である。各サービス空間 7 A，7 B，7 Cには、それぞれオブジェクトリポジトリ 1 A，1 B，1 Cが存在し、これらを管理するためにサービスオブジェクト管理機構 3 0 A，3 0 B，3 0 Cが設けられている。

【0 0 2 1】

なお、1つのサービス空間には任意の数のオブジェクトリポジトリが存在してよい。オブジェクトリポジトリを管理するサービスオブジェクト管理機構の数は任意でよい。1つのサービスオブジェクト管理機構が2以上のオブジェクトリポジトリを管理しても良い。ここでは、一例として、サービスオブジェクトの管理機構とオブジェクトリポジトリとをそれぞれ1組ずつ図示している。

【0 0 2 2】

サービス空間接続管理機構 4 0 Aは、サービスオブジェクト管理機構 3 0 A，3 0 B，3 0 Cを含む各サービス空間の相互接続情報を動的に管理する機能を持つ。その動作の詳細は後で説明するが、この図に示すように、サービス空間接続管理機構 4 0 A，4 0 Bによってサービス空間 7 A，7 B，7 Cが一体となり、例えばサービス検索のためのメッセージがあるサービス空間でサービスオブジェクトの検索に使用された場合、このメッセージがサービス空間を越えて伝搬し、検索に利用される。

【0 0 2 3】

また、サービス空間接続管理機構 4 0 A，4 0 Bは、それぞれサービスオブジェクト管理機構 3 0 A，3 0 B，3 0 C等とのメッセージ通信によってサービス空間の相互接続情報を収集し、更新していく。

【0 0 2 4】

図 3 に、サービスオブジェクト管理機構の構成図を示す。

上記サービスオブジェクト管理機構は、図に示すように、サービスオブジェクト管理機構インタフェース部 31 と、サービスオブジェクト管理機構本体部 32 によって構成される。サービスオブジェクト管理機構インタフェース部 31 は、接続管理インタフェース (I/F) 311 と登録削除更新検索インタフェース 312 とを備える。

【0025】

接続管理インタフェース 311 は、上記サービス空間集中管理機構 10 と接続されて、管理情報を受信し、上記相互接続情報を含む管理情報の送信を行うためのインタフェースである。また、登録削除更新検索インタフェース 312 は、上記サービスオブジェクト検索管理機構 20 と接続されて、サービス利用者の検索メッセージを受け付け、その回答を送信する機能を持つインタフェースである。

【0026】

サービスオブジェクト管理機構本体部 32 は、マルチキャストアナウンス機能部 321、接続管理機能部 322、登録削除更新検索機能部 323、正当性検査機能部 324 及びリポジトリアクセス機能部 325 を備えている。マルチキャストアナウンス機能部 321 は、このサービスオブジェクト管理機構の存在等の情報を定期的に図 1 に示すサービス空間接続管理機構 40 に通知する機能を持つ部分である。

【0027】

具体的には、マルチキャスト機能を利用し、マルチキャスト半径内に所定のメッセージを送信する。マルチキャスト半径というのは、情報を通知すべき範囲を表すための、サービスオブジェクト管理機構を中心とする距離のことである。その決め方は任意であるが、例えば、同一の利用者が利用する確率の高いいくつかのサービス空間を含めた範囲とすればよい。こうして、このサービスオブジェクト管理機構が存在するサービス空間を管理するサービス空間接続管理機構に対してだけでなく、他のサービス空間を管理するサービス空間接続管理機構に対しても、自己の存在を示すメッセージを送信し、相互接続情報を与えるように機能する。

【0028】

接続管理機能部 322 は、後で図 7 を用いて説明するサービス空間の接続管理を実行するために、サービス空間接続管理機構 40 とメッセージ通信を行う部分である。このメッセージは、サービス空間接続管理機構情報 33 を含む。登録削除更新検索機能部 323 は、管理者の要求により、オブジェクトリポジトリ 1 に格納されたサービスオブジェクト 3 や属性情報 5 の登録、削除、更新、検索等を管理する部分である。

【0029】

また、正当性検査機能部 324 は、オブジェクトリポジトリ 1 に格納された各サービスオブジェクト 3 の正当性、即ち、利用可能なサービスオブジェクトであるか、利用不可能なサービスオブジェクトであるかの検査をする機能を持つ部分である。例えば、そのサービスオブジェクトの有効期限が切れた場合には、オブジェクトリポジトリ 1 から、そのサービスオブジェクトを自動的に削除するといった処理も行う。

【0030】

リポジトリアクセス機能部 325 は、登録削除更新検索機能部 323 の依頼等に基づいてオブジェクトリポジトリ 1 に格納されたサービスオブジェクト 3 をアクセスする機能を持つ部分である。

【0031】

図 4 に、サービス空間接続管理機構の構成図を示す。

サービス空間接続管理機構 40 は、サービス空間接続管理機構インタフェース部 41 と、サービス空間接続管理機構本体部 42 とから構成される。サービス空間接続管理機構インタフェース部 41 は、作成インタフェース 411 (I/F)、削除インタフェース 412、更新インタフェース 413、検索インタフェース 414 を備えている。また、サービス空間接続管理機構本体部 42 は、サービスオブジェクト管理機構連携管理機能部 421、接続情報管理機能部 422、一貫性管理機能部 423 を備えている。接続情報管理機能部 422 は、親空間情報 424、子空間情報 425 を記憶している。

【0032】

サービス空間接続管理機構インタフェース部 41 は、担当するサービス空間の

相互接続情報を管理するために、これを作成し、削除し、更新し、検索する機能を持つ部分である。これらのサービス空間接続管理情報は、既に説明した通り、サービスオブジェクト管理機構からメッセージ通信により収集される。

【0033】

サービスオブジェクト管理機構連携管理機能部 421 は、担当する各サービスオブジェクト管理機構 30 のメッセージ通信を受け付けて、これらのサービスオブジェクト管理機構のリストを記憶して、管理する部分である。接続情報管理機能部 422 は、対象となるサービス空間の親子関係や各サービス空間に関する情報を記憶して管理する部分で、例えばここに親空間情報 424 と複数の子空間情報 425 とを記憶している。親空間情報 424 は親となるサービス空間名である。子空間情報 425 は子となるサービス空間名である。子になるサービス空間は複数存在させることができる。子になるサービス空間がない場合もある。

【0034】

一貫性管理機能部 423 は、特定のサービス空間を管理するサービス空間接続管理機構が同時に 2 つ以上存在しないことを保証する機能を持つ。即ち、1 つのサービス空間は 1 つのサービス空間接続管理機構によって管理され、そのサービス空間の内部に存在する全てのサービスオブジェクト管理機構に関する情報が収集され管理される。更に、そのサービス空間と親子関係にある、他のサービス空間に関する情報をサービス空間接続管理機構 40 が持つようにしている。各サービス空間に関する情報の一貫性を維持するためである。なお、2 つ以上のサービス空間を 1 つのサービス空間接続管理機構が管理するようにしても差し支えはない。

【0035】

図 5 に、サービスオブジェクト検索管理機構の構成図を示す。

サービスオブジェクト検索管理機構は、図に示すように、サービスオブジェクト検索管理機構インタフェース部 21 と、サービスオブジェクト検索管理機構本体部 22 とを備える。サービスオブジェクト検索管理機構インタフェース部 21 には、検索インタフェース 23 が設けられている。この検索インタフェース 23 は、サービス利用者から検索メッセージを受け付ける機能を持つ部分である。

【0036】

サービスオブジェクト検索管理機構本体部 22 には、検索処理解釈実行機能部 24 が設けられている。この検索処理解釈実行機能部 24 は、検索メッセージの内容を解釈し、対象となるサービス空間において検索処理を依頼する機能を持つ。例えば、図に示すように、自己の所属するサービス空間 7A のサービスオブジェクト管理機構 30A に対し、この検索メッセージを送信し、該当するサービスオブジェクトの検索を依頼する。また、サービスオブジェクト管理機構 30A の検索結果を受け付けて、その内容を解釈しサービス利用者に送信するメッセージを生成する機能を持つ。

【0037】

また、検索処理解釈実行機能部 24 は、検索を依頼したサービスオブジェクト管理機構 30A から検索に失敗した旨のメッセージを受け付けたとき、サービス空間接続管理機構 40 の持つ情報を利用して、検索メッセージを例えば親子関係にある他のサービス空間 7B, 7C, 7D に送信して、その検索依頼を行う機能を持つ。サービス空間接続管理機構 40 の持つ情報を利用すれば、このようにサービス空間を越えた検索メッセージの送信が可能になり、広範囲に渡るサービスオブジェクトの検索が可能になる。

【0038】

図 6 は、サービス空間集中管理機構の構成図である。

サービス空間集中管理機構 10 は、図に示すように、サービス空間集中管理ツール 11 と、サービス空間集中管理バックエンドサービス 12 を備える。サービス空間集中管理バックエンドサービス 12 は、相互接続情報収集機能部 13 と、相互接続作成削除変更機能部 14 と、サービス空間作成削除変更機能部 15 を備えている。これによって、サービス空間集中管理機構 10 は、全てのサービス空間のライフサイクルと相互接続に関する管理機能を実現する。

【0039】

即ち、サービス空間接続管理機構 40 とメッセージ通信を行うことによって、新たなサービス空間の作成、不要なサービス空間の削除や変更を行う。また、相互接続情報収集機能部 13 は、サービス空間接続管理機構 40 の情報を収集し、

サービス対象となる全てのサービス空間と各サービス空間の関係を示す相互接続情報を集積しておく。相互接続情報等の作成、削除、変更管理は、この相互接続情報収集機能部 1 3 により収集された情報に基づいて実行される。

【0 0 4 0】

また、サービス空間作成削除変更機能部 1 5 は、各サービス空間のサービスオブジェクト管理機構 3 0 と通信を行い、サービス空間の作成、削除、変更等の制御を行う。即ち、サービス空間集中管理バックエンドサービス 1 2 には、全てのサービスオブジェクト管理機構と、これらのサービスオブジェクト管理機構が所属するサービス空間及び各サービス空間の相互接続情報が収集され一元管理が行われている。

【0 0 4 1】

なお、これらの情報は、図 1 に示すサービス空間集中管理機構 1 0 とサービス空間接続管理機構 4 0 とのメッセージ通信により行われる。また、サービス空間の相互接続変更等は、サービス空間集中管理機構 1 0 からの要求によりサービス空間接続管理機構 4 0 が行い、その相互接続情報がサービス空間集中管理機構 1 0 とサービス空間接続管理機構 4 0 との間のメッセージ通信により収集される構成となっている。以下、本発明のシステムの動作を説明する。

【0 0 4 2】

図 7 には、サービス空間接続管理機構の動作説明図を示す。

この図を用いて、サービス空間接続管理機構 4 0 が、担当するサービス空間の相互接続情報を収集し管理するフェーズの内容を説明する。図中、このフェーズにおける各動作を時間順に S 1，S 2，…S 6 というように図示した。この例は、親サービス空間 7 A と子サービス空間 7 C とが存在し、新たに、サービス空間 7 B と、このサービス空間に存在するサービスオブジェクトを管理するサービスオブジェクト管理機構 3 0 B と、サービス空間接続管理機構 4 0 B とが生成されたときの動作を示す。

【0 0 4 3】

はじめに、サービスオブジェクト管理機構 3 0 B は、自己の存在を通知するためサービス空間接続管理機構 4 0 B に、メッセージ M を送信する。これにより、

サービス空間接続管理機構 40B に、サービスオブジェクト管理機構 30B が登録されて、その後の管理対象となる（ステップ S1）。また、これで、サービス空間接続管理機構 40B は、サービス空間 7B の管理を担当することを認識する。サービス空間接続管理機構 40B は、サービスオブジェクト管理機構 30B に対して、サービス空間 7B の管理を担当することを通知するために、メッセージ M を返す（ステップ S2）。

【0044】

次に、サービス空間接続管理機構 40B は、このようなイベントの発生を、他のサービス空間の管理を担当するサービス空間接続管理機構 40A に通知するため、サービスオブジェクト管理機構 30B に対しイベント通知の発行を依頼する（ステップ S3）。この依頼を受けて、サービスオブジェクト管理機構 30B は、サービス空間 7A 中のサービスオブジェクトを管理するサービスオブジェクト管理機構 30A に対し、自己の存在を示すメッセージ M を送信する。メッセージ M を受信したサービスオブジェクト管理機構 30A は、そのメッセージ M を、親サービス空間 7A を担当するサービス空間接続管理機構 40A に転送する（ステップ S4）。

【0045】

サービス空間接続管理機構 40A は、受信したメッセージ M を子空間のものと判定して、サービス空間 7B を子空間情報に登録する。これで、サービス空間 7A とサービス空間 7B との親子関係が成立する。このように、新規登録要求を送信した側が子空間、受信した側が親空間とになるように規則を決めておけば、自動的に親子関係が成立する。また、親子関係は、メッセージに含まれる別の情報により決定するようにしても構わない。

【0046】

親子関係が決まると、サービス空間接続管理機構 40A は、すでに管理対象として登録されているサービスオブジェクト管理機構 30A を通じて、親サービス空間 7A の登録を要求するメッセージ P を、サービス空間接続管理機構 40B に送信する。サービス空間接続管理機構 40B は、メッセージ P を受信して、サービス空間 7A を親空間情報に登録する（ステップ S5）。

【0047】

以上の動作によって、サービス空間7Aのサービス空間接続管理機構40Aと、サービス空間7Bのサービス空間接続管理機構40Bとが、それぞれ親子関係である旨を示す親空間情報と子空間情報を獲得してリンクされる。例えば、一方のサービス空間で検索メッセージを受け付けた場合に、親から子へ、あるいは子から親へそのメッセージを転送する接続関係が確立する。

【0048】

上記のように、あるサービスオブジェクト管理機構に何らかの状態変化が発生した場合に、サービスオブジェクト管理機構からサービス空間接続管理機構に対しメッセージが送信される。このメッセージの内容に従って、サービス空間接続管理機構は、自己が管理を担当するサービス空間や、親子関係にあるサービス空間のサービス空間接続管理機構と接続管理情報を交換し、自己の親空間情報や子空間情報等を更新する。以上の動作により、サービス空間接続管理機構中に、サービスオブジェクト管理機構のリストと、親空間情報と、子空間情報とが登録され、各空間の接続関係を明らかにするための情報が集まる。

【0049】

また、サービスオブジェクト管理機構は、それぞれ既に説明したように、例えば一定時間おきにマルチキャストアナウンス機能を用いて、自己の状態をメッセージによって近接するサービス空間接続管理機構に伝える。もちろん、サービスオブジェクト管理機構は、マルチキャスト半径内に含まれていない特定のサービス空間を指定して、メッセージを送信するようにしても良い。図7のステップS6は、このようなメッセージCによって、サービス空間接続管理機構40Bがサービスオブジェクト管理機構30Cを含むサービス空間7Cを子空間として登録した動作を示す。これは、メッセージCを受信した側が親空間になった例である。

【0050】

更に、各サービスオブジェクト管理機構は、マルチキャストアナウンスのみならず自己の状態変化に基づくイベントが発生した場合に、その都度近接するサービス空間を担当するサービス空間接続管理機構に対し自己の状態を通知する。こ

のようなメッセージ通信によって、各サービス空間接続管理機構は、全てのサービス空間のサービスオブジェクト管理機構の状態や相互接続関係を明らかにし、円滑なディレクトリサービスを実現する。

【0051】

図8には、図5に示したサービスオブジェクト検索管理機構に入力するサービス検索メッセージの内容説明図を示す。

この図に示すような構成の検索メッセージを用いて、上記のようなディレクトリ管理システムを利用した検索サービスが実現される。検索メッセージ51には、サービスオブジェクト属性値リスト52、サービスオブジェクト型55及び検索個数上限値56が含まれる。

【0052】

サービスオブジェクト属性値リスト52は、サービスオブジェクトを検索するために必要な属性値を表現したデータである。即ち、サービスオブジェクトの検索のために、検索キーをアンド条件やオア条件等で結んだ検索式がその内容とされる。属性名53は例えばディレクトリやフォルダ名で、属性値は例えばファイル名やキーワードやワイルドカードを含めたキーである。属性名53や属性値54の内容や、その数は任意である。従来より、インターネットを利用して情報検索をする場合と同様でよい。

【0053】

サービスオブジェクト型55は、サービスオブジェクトがどのクラス型を元に作成されたものであるかを指定するためのものである。検索個数上限値56は、検索結果の情報量を制限するためのパラメータである。上記のように、サービス空間をサービス空間接続管理機構で相互接続すると、多量の検索結果が出力されることがあるので、検索時間を制限するためにもこのような方法がこのましい。以上のような検索メッセージが、図5に示す検索インタフェース23を通じて検索処理解釈実行機能部24に受信されると、対象となるサービス空間のサービスオブジェクト管理機構30Aに対し、その検索が依頼される。

【0054】

サービスオブジェクト管理機構30Aは、図3に示したようなりポジトリアク

セス機能部 3 2 5 によってオブジェクトリポジトリ 1 を検索し、属性値の一致する属性情報を持つサービスオブジェクト 3 を抽出する。この結果は、図 5 に示した検索処理解釈実行機能部 2 4 に返され、必要に応じて他のサービス空間の検索が実行される。

【0 0 5 5】

なお、検索対象となるサービス空間を拡張していく場合、例えば子から親に向かう方向あるいは親から子に向かう方向と言うように方向を決めておけば良い。最初に検索対象となったサービス空間と親子関係にある他のサービス空間と、それより遠い関係にあるサービス空間であって、例えば二親等とか三親等といった距離を設定し、検索範囲を決めておくのもよい。具体的に検索対象のサービス空間名を指定しておくのもよい。検索範囲の決定は、サービス空間接続管理機構の持つ情報を利用して行われる。

【0 0 5 6】

サービスオブジェクト検索管理機構は、こうして決定した検索範囲のサービス空間にあるサービスオブジェクト管理機構に、検索依頼のためのメッセージを一斉に送信する。検索依頼を受けた各サービスオブジェクト管理機構は、それぞれ独自に検索を実行する。検索メッセージ 5 1 に含まれた検索個数上限値 5 6 を超える個数のサービスオブジェクトが抽出された場合には、サービスオブジェクト管理機構は検索処理を中止し、検索結果を検索処理解釈実行機能部 2 4 に返す。これによって、サービスオブジェクト検索管理機構は、予め決定したサービス空間における、検索結果を収集して、利用者にその結果を報告する。

【0 0 5 7】

なお、上記のサービス空間集中管理機構、サービスオブジェクト検索管理機構、サービス空間接続管理機構、オブジェクトリポジトリ等は、それぞれネットワーク上の任意のコンピュータやその他の端末装置上に分散配置され、それぞれ分担して必要な役割を実行することが好ましい。各機構は、いずれも一体にされても別々に存在してもよい。また、その一部をハードウェアにより形成されてもよい。

【0 0 5 8】

＜具体例 1 の効果＞

上記のように、サービスオブジェクトを格納したオブジェクトリポジトリを管理するサービスオブジェクト管理機構とサービス空間接続管理機構とが、それぞれメッセージ通信によって相互接続情報を交換し、ネットワークによって接続された分散したサービス空間の関係や状態を常に反映するように構成したので、定期的に登録、更新、削除がされるネットワーク環境で、サービスオブジェクトの変化等に効率よく対応するディレクトリサービスを提供することが可能になる。

【0059】

また、検索メッセージに対してもサービス空間接続管理機構の持つ情報によって、サービス空間を越えて他のサービス空間に対し検索メッセージを送信し、広範囲な情報収集を自動的に行うことが可能になる。

【0060】

＜具体例 2＞

この具体例では、アクセス権を持つ利用者だけにサービスオブジェクトの検索を認めるようなサービス空間が存在する場合の認証機構を提供する。

【0061】

図 9 には、具体例 2 の分散ディレクトリ管理システム主要部構成図を示す。

この図の右側に示す部分は図 1 と同様の構成で、ここにディレクトリ管理認証機構 60 を新たに設けた点が特徴である。ディレクトリ管理認証機構 60 は、サービスオブジェクト検索管理機構 20 やサービスオブジェクト管理機構 30、サービス空間接続管理機構 40 との間の暗号化されたあるいは署名付きのメッセージ通信を実現して、サービス利用者の認証を行い、アクセス権のある利用者のみディレクトリサービスを提供する機能を持つ。

【0062】

図 10 には、ディレクトリ管理認証機構の具体的な構成図を示す。

このディレクトリ管理認証機構 60 は、ディレクトリアクセス認証チケット管理機能部 61 と、公開鍵秘密鍵管理機能部 62 と、デジタル署名管理機能部 63 と、アクセスコントロール管理機能部 64 とを備える。公開鍵秘密鍵管理機能部 62 は、認証用鍵リポジトリ 65 を備え、ここに公開鍵や秘密鍵を格納する。

【0063】

公開鍵や秘密鍵は、サービスオブジェクト利用者の認証のために使用される。例えば、利用者が自己の秘密鍵を用いて検索要求メッセージに署名を行うと、ディレクトリ管理認証機構 60 は、その利用者の公開鍵を用いて署名の存在を確認し、その利用者がディレクトリサービスを受けることができる者かどうかの認証を行うことができる。また、例えば、ディレクトリ管理認証機構 60 が利用者の公開鍵を用いて暗号化したデータは、その秘密鍵を所有する利用者のみが解読できる。故に、アクセス権を持つ特定の利用者によりのみ検索結果を提供できる。

【0064】

ディレクトリアクセス認証チケット管理機能部 61 は、ディレクトリサービスを利用するためのチケットを利用者に発行し、利用者からチケットの提出があった場合、その正当性を検証する機能を持つ。デジタル署名管理機能部 63 は、デジタル署名を実行し、あるいはデジタル署名されたデータを確認する機能を持つ。

【0065】

アクセスコントロール管理機能部 64 は、ディレクトリアクセス認証チケット管理機能部 61、公開鍵秘密鍵管理機能部 62、デジタル署名管理機能部 63 等の認証処理の結果を受けて、サービス空間接続管理機構 40 の相互接続情報交換やサービスオブジェクト検索の際のアクセスコントロールを行う。これによって、例えばアクセス権の無い利用者の利用を禁止し、適切なサービスを提供する。

【0066】

図 11 に、具体的な認証機構を利用したサービス空間における接続管理機構の動作説明図を示す。

まず、各サービスオブジェクト管理機構やサービス空間接続管理機構は、それぞれディレクトリ管理認証機構 60 の公開鍵秘密鍵管理機能部 62 から公開鍵や秘密鍵を入手し、送信するメッセージにデジタル署名を行い、あるいはメッセージの暗号化を行う。これによって、限定されたサービス空間以外にメッセージは通知されず、また限定されたサービス空間以外にそのメッセージを利用される

ことがない。

【0067】

図11に示した動作は、図7に示したものと対応している。そのステップS1～ステップS5の部分の動作は、図7のケースと変わらない。即ち、サービス空間接続管理機構40Aとサービス空間接続管理機構40Bとは、それぞれサービスオブジェクト管理機構30Aやサービスオブジェクト管理機構30Bとのメッセージ通信によって自空間の状態と親空間情報や子空間情報の登録を実行する。

【0068】

子サービス空間7Cにおけるサービスオブジェクト管理機構30Cとサービス空間接続管理機構40Cも、同様の手順によって、図7で説明した通りの情報の登録等を実行する。このとき、各メッセージにデジタル署名がなされていれば、そのメッセージを受信した機構は、それぞれメッセージの信頼性を確認し、相互接続情報の整備を行う。これによって、誤った相互接続情報の受信により、サービス空間接続管理機構の機能が妨げられるのも防止できる。サービスオブジェクト管理機構とサービス空間接続管理機構とのメッセージ通信を暗号化したり、署名を要求したりする方法は、例えば、図に示すサービス空間7A、7B、7Cがいずれも、図示しない他のサービス空間と隔離されて、特定の利用者にのみアクセス権を与えるような場合に適する。

【0069】

次に、検索管理機構による上記認証機構の利用について説明をする。アクセス権を持つ利用者から検索メッセージを受信すると、図5に示した検索処理解釈実行機能部24は、図9に示したディレクトリ管理認証機構60に対し、検索メッセージへの署名を依頼する。利用者のアクセス権の有無は、サービスオブジェクト検索管理機構20の側で判定する。ここではサービス空間単位でアクセス権が与えられている。検索メッセージへの署名は、そのサービスオブジェクト検索管理機構20と同一のサービス空間で署名認証を管理するディレクトリ管理認証機構60が行う。そして、検索対象となる別のサービス空間のディレクトリ管理認証機構60に対して、署名された検索メッセージを送信する。

【0070】

検索メッセージを受け取ったディレクトリ管理認証機構 60 は、その署名の正当性を確認し、アクセス権を持つサービス空間からのメッセージであるかどうかを判断する。アクセス権の無いサービス空間からのメッセージの場合には、送信元にサービスオブジェクトのアクセスを許可しない旨を通知し、処理を終了する。アクセス権のあるサービス空間からのメッセージと判断された場合には、ディレクトリ管理認証機構 60 は、該当するサービスオブジェクト管理機構に対して、その検索処理を依頼する。その後の検索結果の通知処理は、これまでの例と同様、依頼元に対しメッセージ通信を用いて行われる。検索結果を含むメッセージを暗号化して送信しても良い。なお、この例では、アクセス権は、サービス空間全体に対して与えられ、そのサービス空間で管理されている利用者は全てアクセス権を持つものとする。

【0071】

一方、サービス空間毎でなく、利用者毎にアクセス権を与える場合には、次のようにする。まず、アクセスに先立ち、該当する利用者アクセス用のチケットを発行する。このチケットには、例えばチケット発行サービス空間、チケット有効サービス空間、発信元有効期間、サービスオブジェクトの利用者名、利用者の公開鍵、ディレクトリ管理認証機構の署名等が含まれる。利用者毎のチケット発行は次のように行われる。

【0072】

まず、利用者の要求により、その利用者を管理するサービスオブジェクト検索管理機構 20 がディレクトリ管理認証機構 60 に対しチケットの要求メッセージを送信する。ディレクトリ管理認証機構 60 は、その利用者名を元に、図 10 に示した認証用鍵リポジトリ 65 から、利用者の公開鍵を抽出する。ディレクトリ管理認証機構 60 は、チケットを生成し、そのチケットを利用者の公開鍵を用いて暗号化する。

【0073】

ディレクトリ管理認証機構 60 は、暗号化したチケットを発信元のサービスオブジェクト検索管理機構 20 に対して送信する。これによって、利用者は、チケットを発行したディレクトリ管理認証機構 60 の所属するサービス空間における

サービスオブジェクトの検索資格を得る。

【0074】

この利用者は、該当するサービスオブジェクトの検索を希望する場合、検索メッセージとチケットとをサービスオブジェクト検索管理機構20に送信する。サービスオブジェクト検索管理機構20は、この検索メッセージとチケットを受信し、検索処理解釈実行機能部24を通じて、対象となるサービス空間のディレクトリ管理認証機構60に送信する。そのディレクトリ管理認証機構は、チケットの正当性を検証し、チケットが正しい場合、サービスオブジェクト管理機構30に検索メッセージを送信し、検索を依頼する。

【0075】

検索が成功した場合には、サービスオブジェクト管理機構30は、その結果をディレクトリ管理認証機構60に通知する。ディレクトリ管理認証機構60は、検索結果を利用者の公開鍵を用いて暗号化した後、サービスオブジェクト検索管理機構20を通じて利用者に送信する。

【0076】

認証機構を用いた例をいくつか説明したが、いずれの場合においても、各機構がそれぞれメッセージ通信を行う際に、公開鍵、秘密鍵を用いてメッセージを暗号化処理したり、メッセージに署名をすることによって、そのメッセージを読むことを許可された機構のみが該当する処理を実行する。こうして、具体例1で説明した分散管理システムの一部について、そのセキュリティを高め、利用制限等を行うことが可能になる。なお、上記ディレクトリ管理認証機構は、サービス空間単位で設けられていても良いし、サービスオブジェクト管理機構単位で設けられていても差し支えない。

【0077】

〈具体例2の効果〉

以上のように、サービス空間接続管理機構を具体例1のシステムに追加することによって、秘密鍵、公開鍵等を用いたメッセージの認証や暗号化によって、相互接続情報を安全確実に管理することが可能になる。更に、サービスオブジェクトの検索においては、許可を受けた利用者によりのみ所定のサービス空間の検索を許

可し、ガードの固いセキュリティ機構による安全な効率的な検索処理を実行することが可能になる。

【0 0 7 8】

なお、上記の具体例では、J A V A 言語環境におけるオブジェクト表現を用いて、各機構を実現する例を示したが、他のC++言語といったオブジェクト指向言語環境によって同様のシステムを実現することが可能である。また、サービスオブジェクトを格納する機構としてオブジェクトリポジトリを用いたが、オブジェクトは別のメモリ上に記憶させ、オブジェクトに関する属性情報のみをデータベース化してオブジェクトリポジトリに保存するような構成を採用しても差し支えない。

【0 0 7 9】

更に、認証機構としては、公開鍵、秘密鍵といった鍵を利用するシステムの他、パスワードやその他の暗号化アルゴリズムを用いたシステムとしても差し支えない。

【図面の簡単な説明】

【図 1】

具体例 1 の分散ディレクトリ管理システム主要部構成図である。

【図 2】

分散ディレクトリ管理システム全体の構成図である。

【図 3】

サービスオブジェクト管理機構の構成図である。

【図 4】

サービス空間接続管理機構の構成図である。

【図 5】

サービスオブジェクト検索管理機構の構成図である。

【図 6】

サービス空間集中管理機構の構成図である。

【図 7】

サービス空間接続管理機構の動作説明図である。

【図 8】

サービス空間におけるサービス検索メッセージの説明図である。

【図 9】

具体例 2 の分散ディレクトリ管理システム主要部構成図である。

【図 10】

ディレクトリ管理認証機構の構成図である。

【図 11】

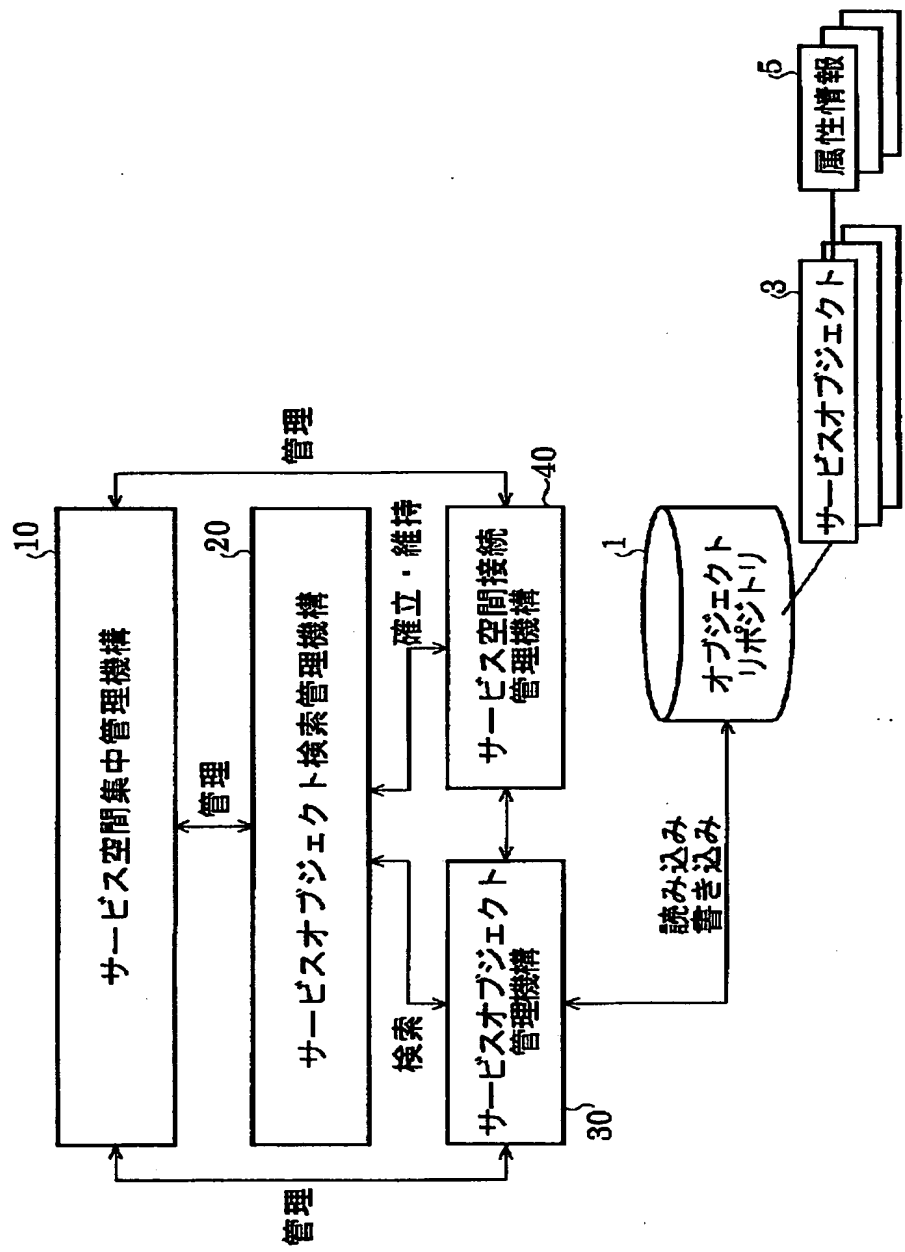
認証機構を利用したサービス空間における接続管理機構の動作説明図である。

【符号の説明】

- 1 オブジェクトリポジトリ
- 3 サービスオブジェクト
- 5 属性情報
- 10 サービス空間集中管理機構
- 20 サービスオブジェクト検索管理機構
- 30 サービスオブジェクト管理機構
- 40 サービス空間接続管理機構

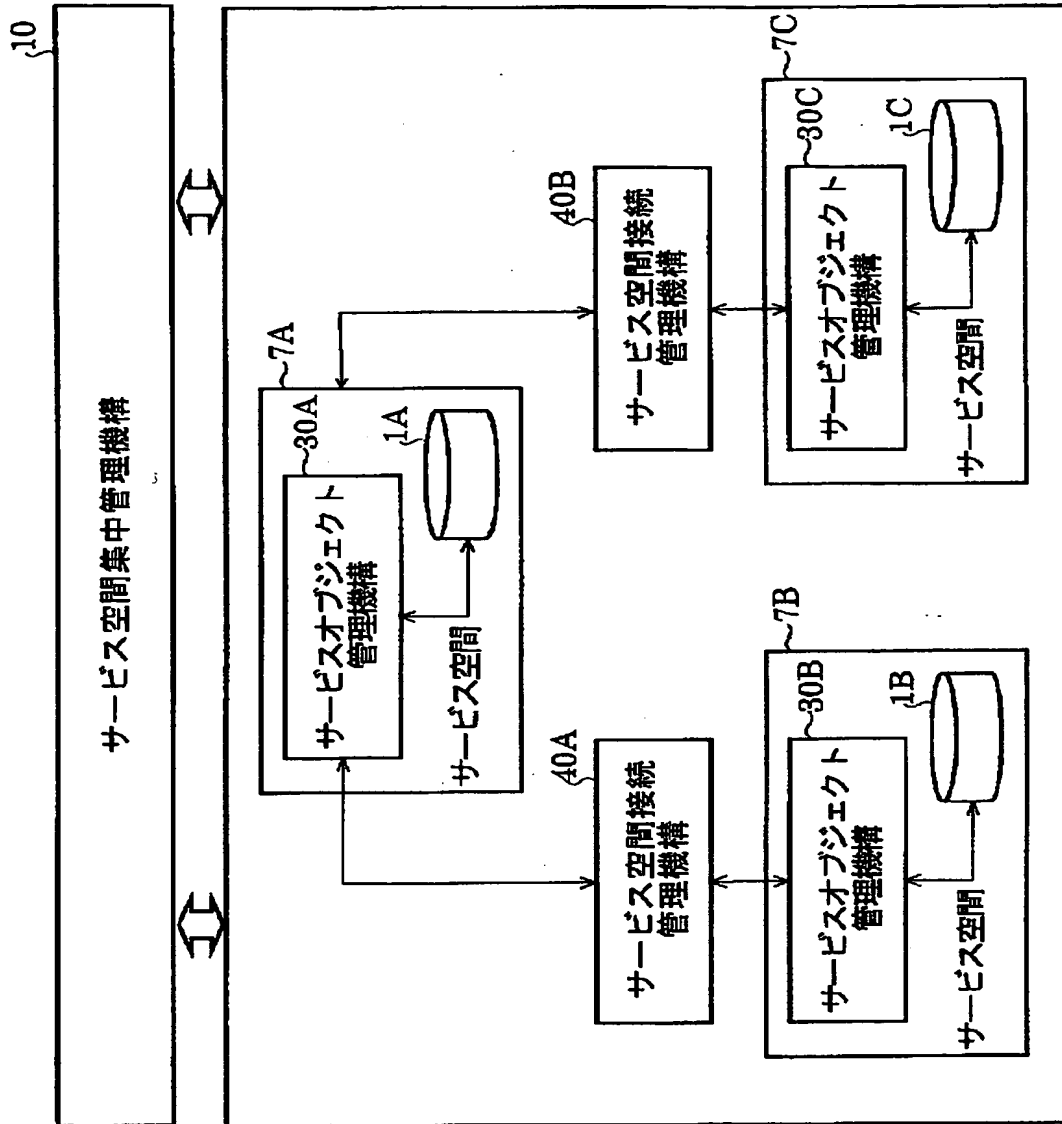
【書類名】 図面

【図 1】



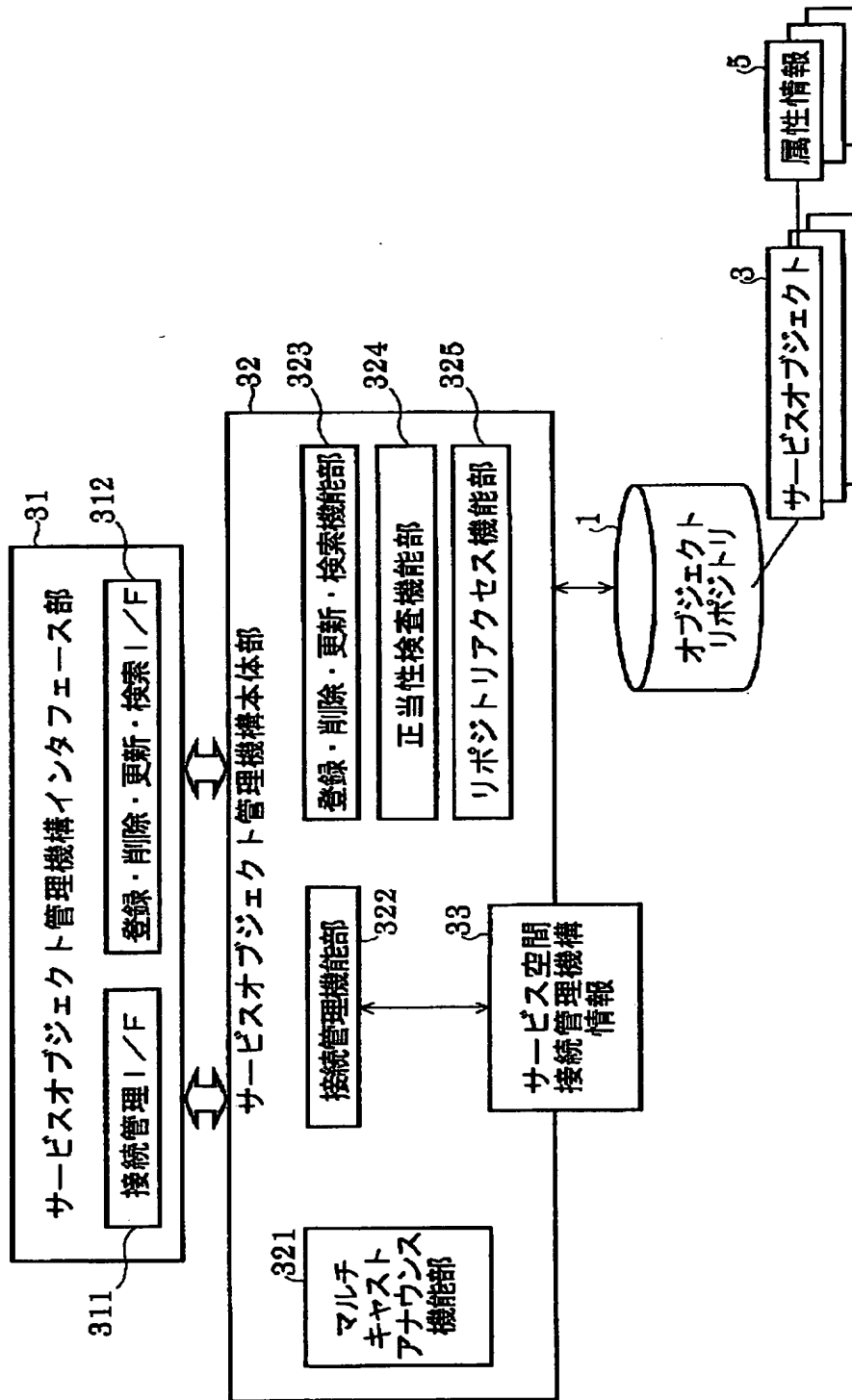
具体例 1 の分散ディレクトリ管理システム主要部構成図

【図 2】



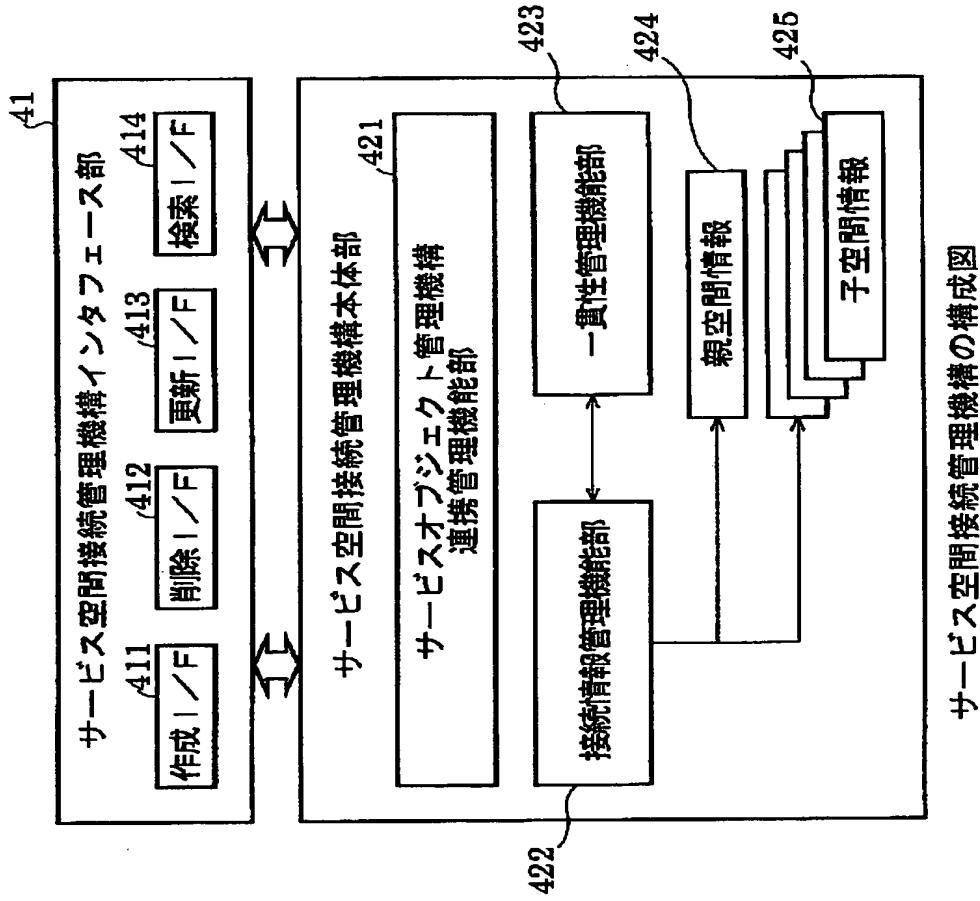
分散ディレクトリ管理システム全体の構成図

【図 3】

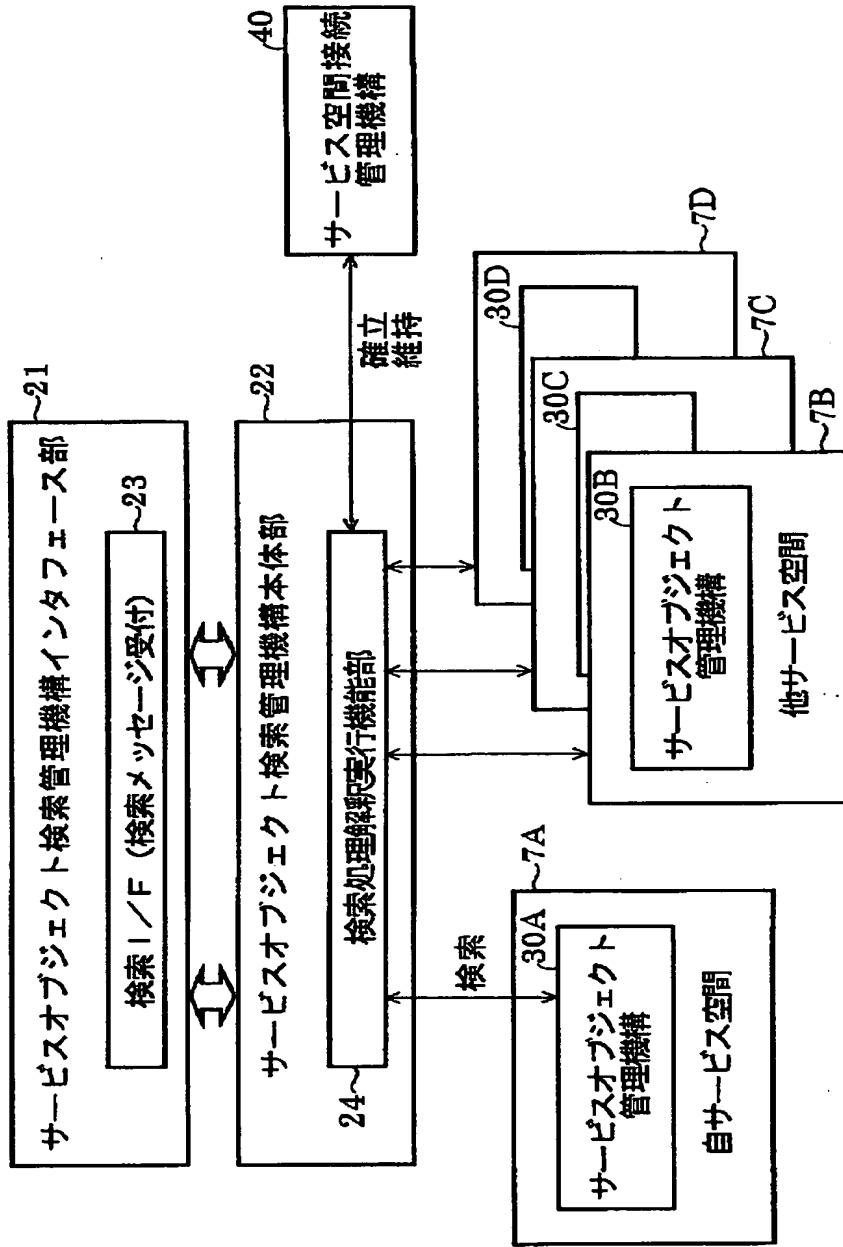


サービスオブジェクト管理機構の構成図

【図 4】

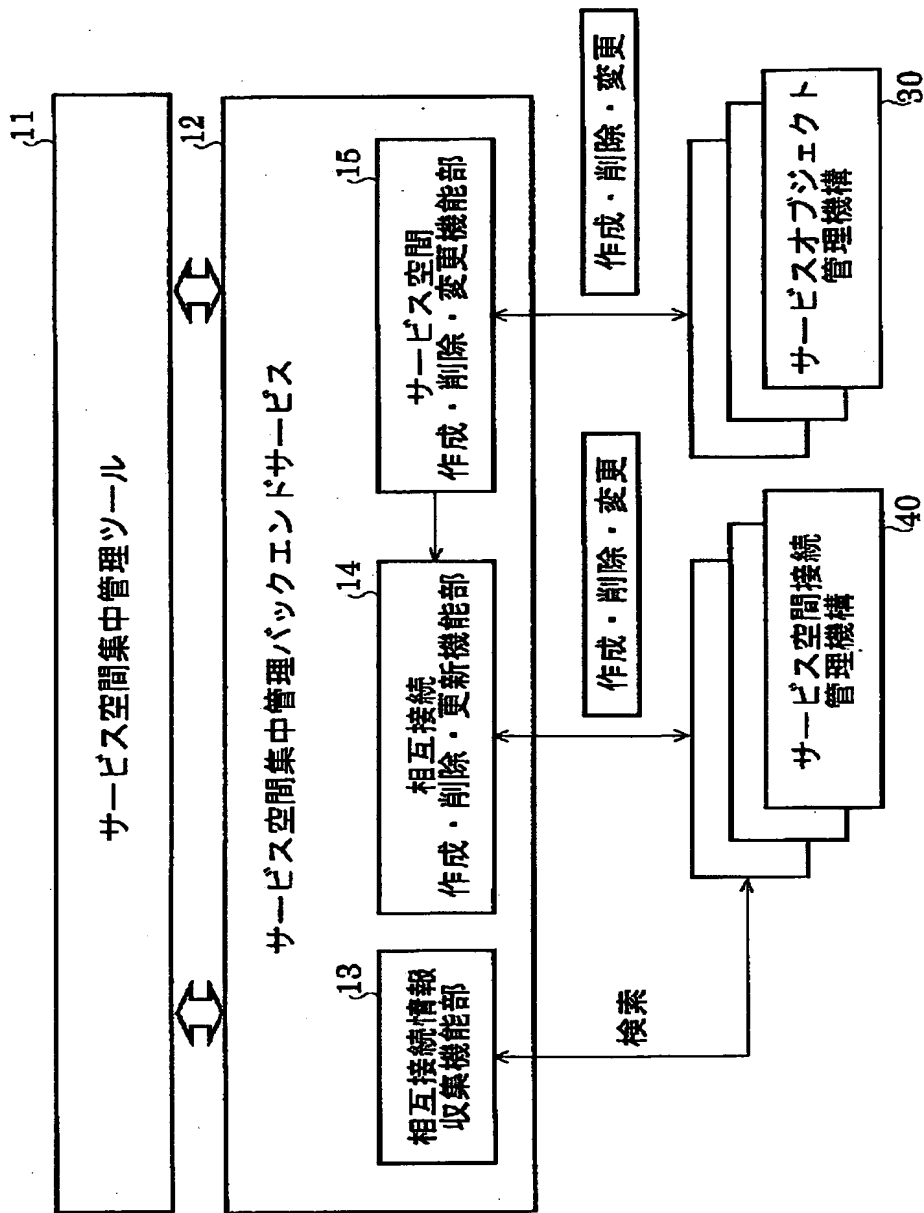


【図 5】



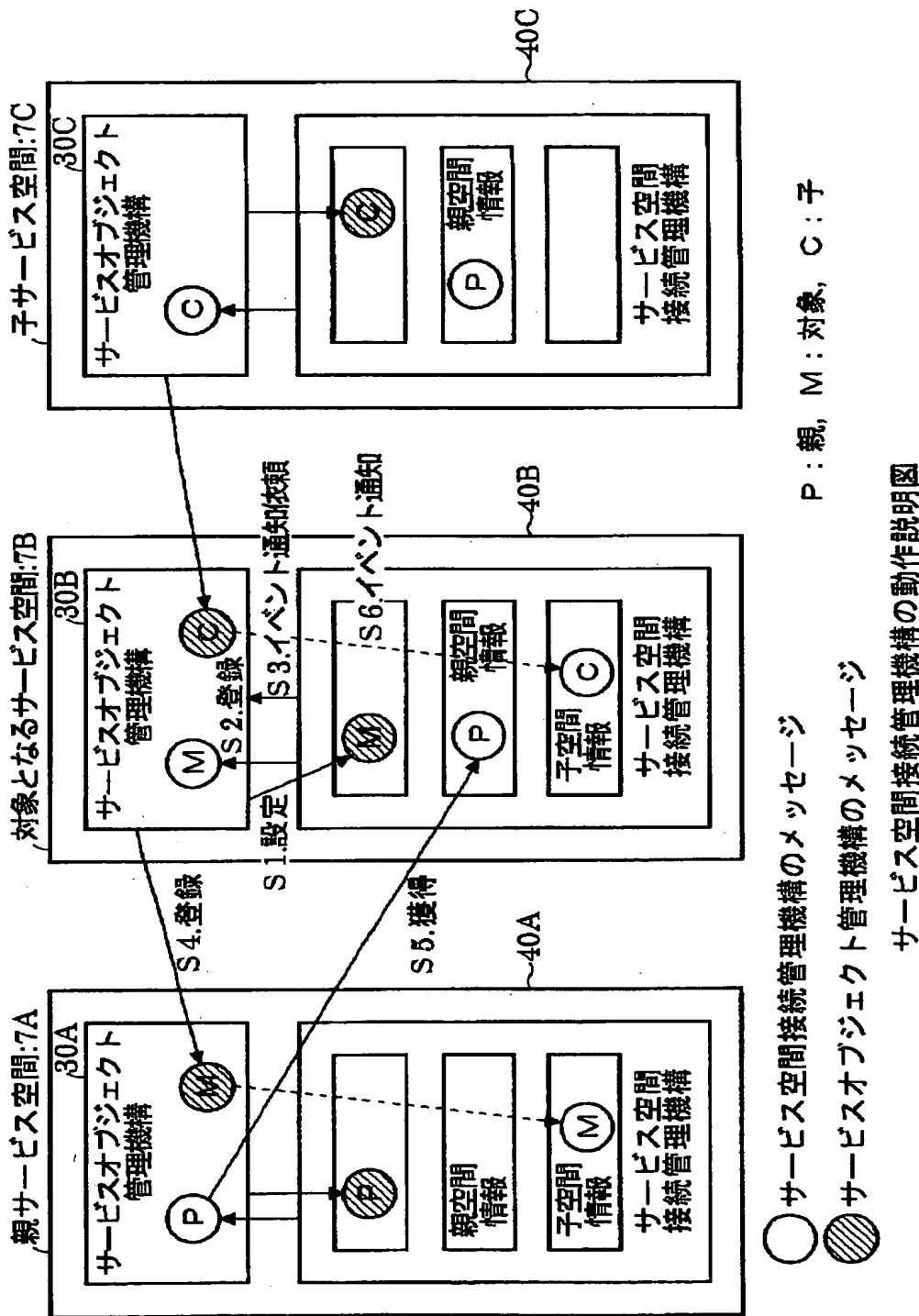
サービスオブジェクト検索管理機構の構成図

【図 6】

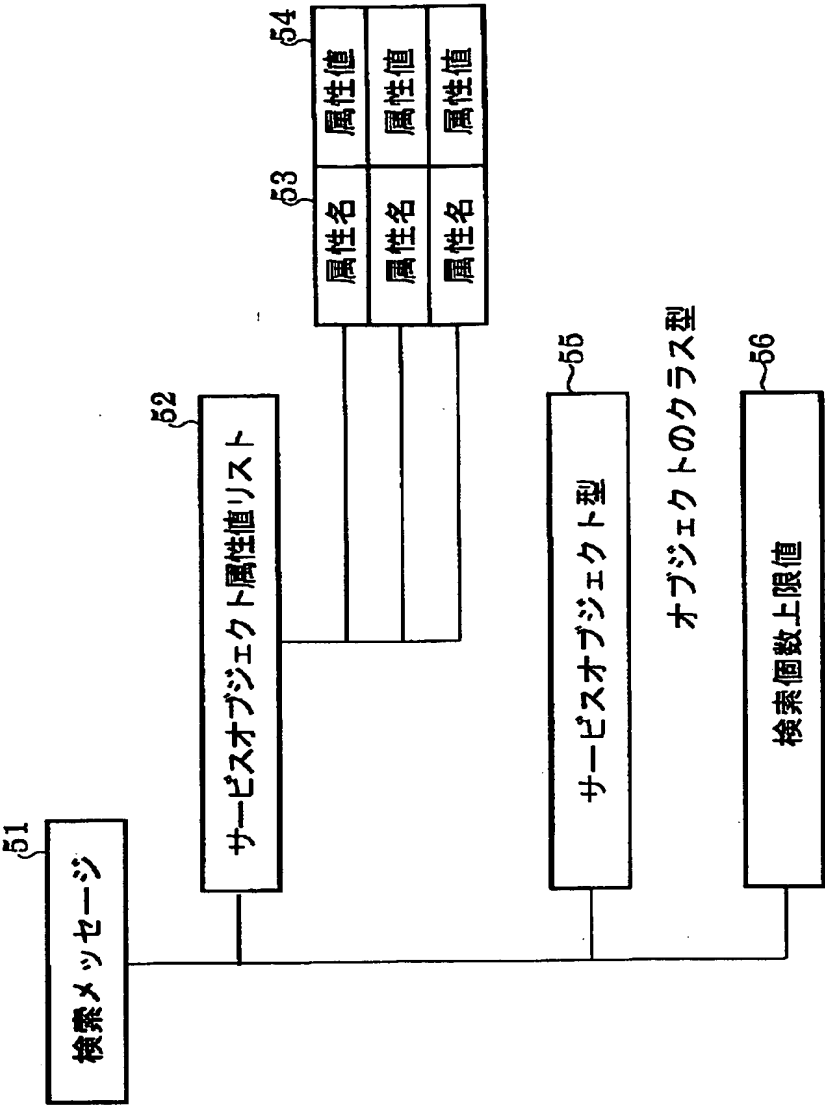


サービス空間集中管理機構の構成図

【図 7】

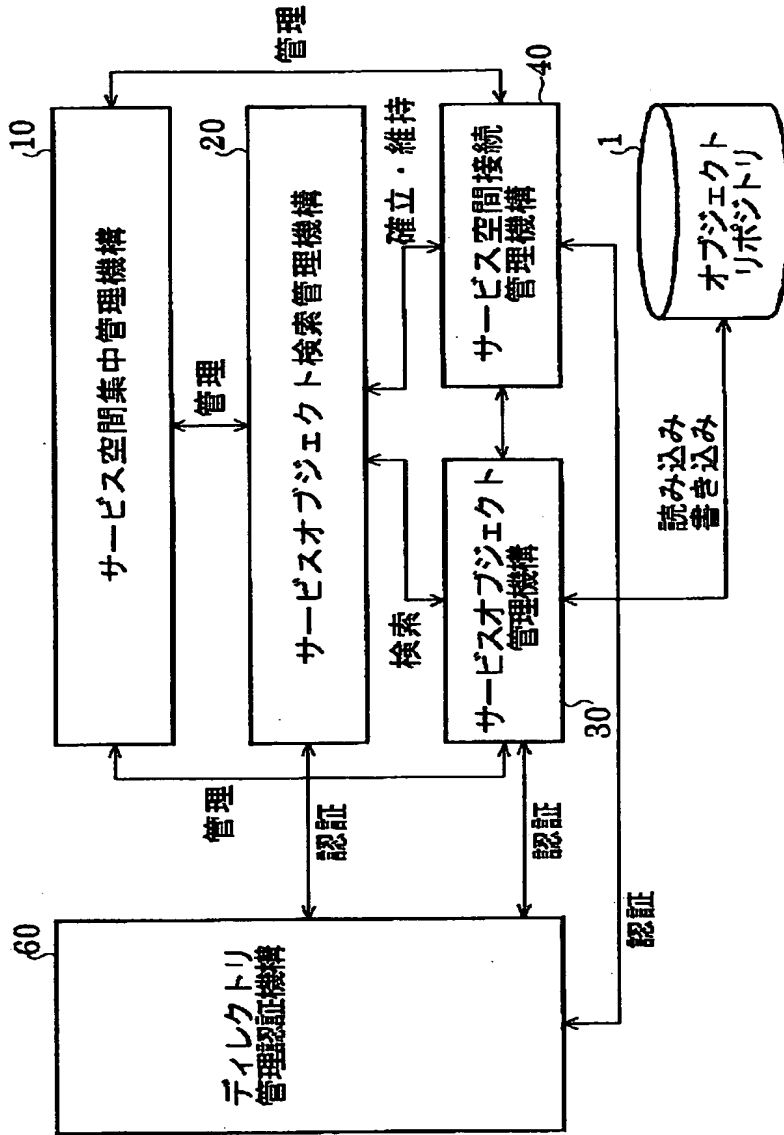


【図 8】



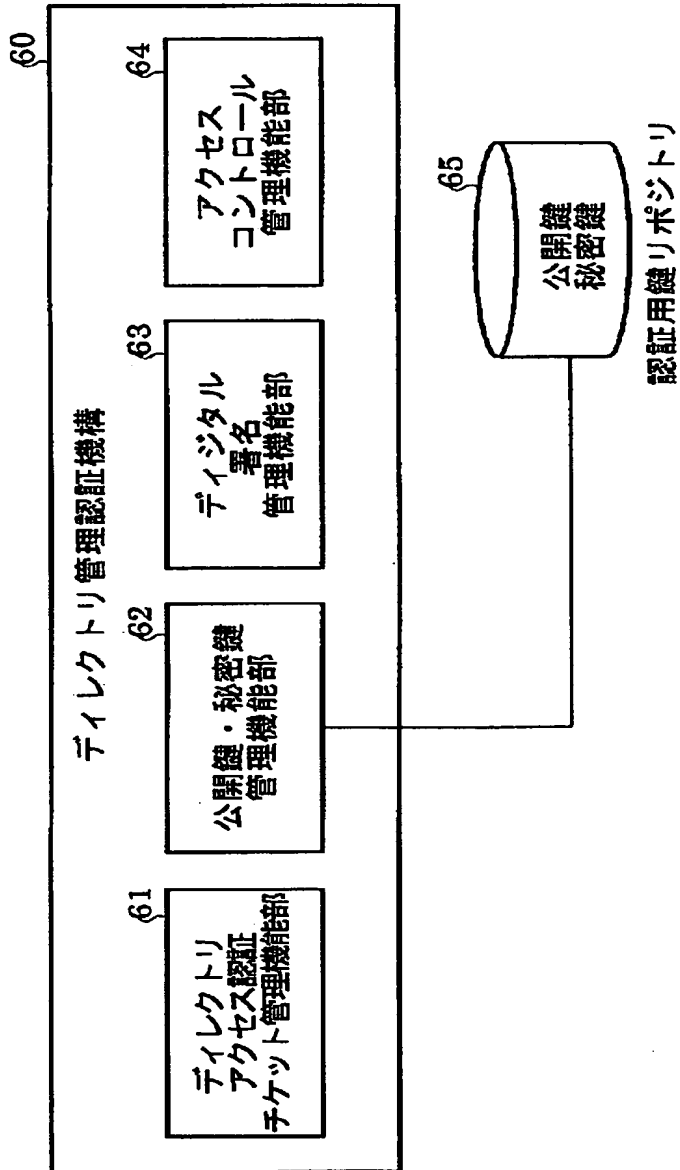
サービス空間におけるサービス検索メッセージの説明図

【図 9】



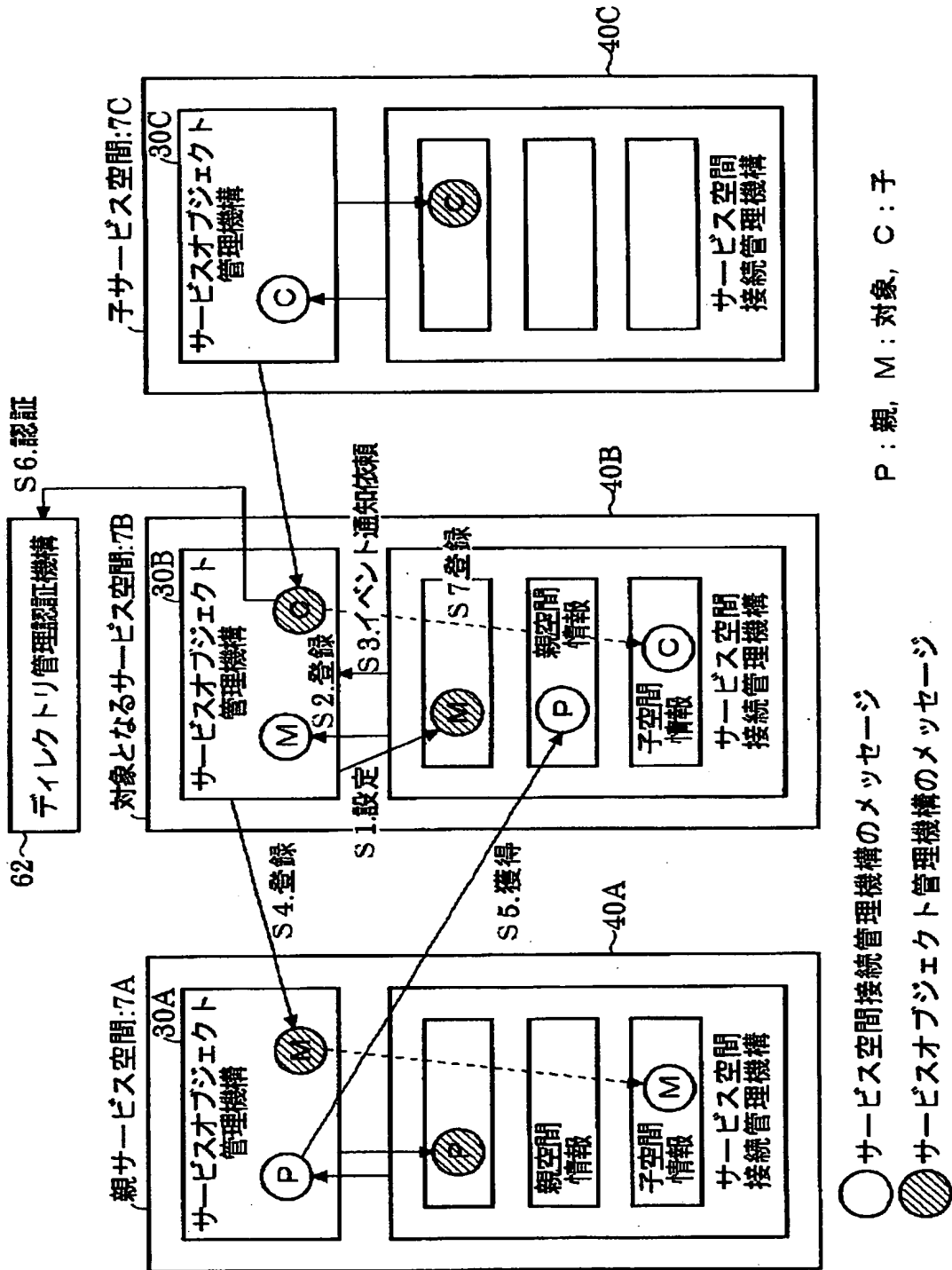
具体例 2 の分散ディレクトリ管理システム主要部構成図

【図 10】



ディレクトリ管理認証機構の構成図

【図 1 1】



認証機構を利用したサービス空間における接続管理機構の動作説明図

【書類名】 要約書

【要約】

【解決手段】 オブジェクトリポジトリ 1 には、サービスオブジェクト 3 や属性情報 5 が格納される。サービスオブジェクト管理機構 30 は、オブジェクトリポジトリ 1 を管理し、ネットワーク上で属性情報 5 をキーとするサービスオブジェクト 3 の検索処理を実行する。サービス空間接続管理機構 40 は、各サービス空間のサービスオブジェクト管理機構 30 とメッセージ通信を行い、各サービス空間の相互接続情報を収集管理する。サービスオブジェクト検索管理機構 20 は、サービスオブジェクト管理機構 30 にサービス利用者からの検索メッセージを送信し、検索結果を得る。検索に失敗した場合には、他のサービスオブジェクト管理機構に改めて検索を依頼する。

【効果】 各機構を J A V A 等のインスタンスオブジェクトで実現すれば、ネットワークディレクトリサービスの動的な管理が可能になる。

【選択図】 図 1

認定・付加情報

特許出願の番号	平成11年 特許願 第049346号
受付番号	59900172499
書類名	特許願
担当官	第七担当上席 0096
作成日	平成11年 3月 3日

<認定情報・付加情報>

【提出日】	平成11年 2月26日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000000295]

1. 変更年月日 1990年 8月22日

[変更理由] 新規登録

住 所 東京都港区虎ノ門1丁目7番12号

氏 名 沖電気工業株式会社